Guía del Autoestopista en Internet, RFC 1118, Ed Krol, Septiembre de 1989.

[N.d.T]: Originalmente publicada en 1987 y editada en forma de Circular de Propuesta RFC 1118, la "Guía del Autopista en Intenet" fue escrita por el Administrador de Red de Supercómputo de la Universidad de Illinois Ed Krol a instancias de la Fundación Nacional de las Ciencias de los EE.UU. Representa la primer guía popular de usuarios de la historia y uso de la red Internet.

Guía del Autoestopista en Internet

Estado de este Memorándum

Este RFC se distribuye a los miembros de la comunidad de Internet para ofrecer algunas sugerencias que permitan a los nuevos participantes de la red comprender cómo se define el rumbo de Internet, cómo obtener información en línea y cómo ser un buen vecino en Internet. Si bien la información presentada puede no ser relevante para los problemas de investigación de Internet, puede ser de interés para diversos investigadores e implementadores. Este memorando no define ni especifica estándares. **Su distribución es ilimitada**.

AVISO:

La Guía del Autoestopista en Internet es un memorando editado de forma muy irregular y contiene muchos pasajes que, en su momento, a sus editores les parecieron una buena idea. Es un complemento indispensable para quienes desean comprender la vida en una Internet infinitamente compleja y confusa. Si bien no puede aspirar a ser útil ni informativo en todos los aspectos, sí ofrece la tranquilizadora afirmación de que, cuando es inexacto, al menos lo es definitivamente. En caso de discrepancia importante, siempre es la realidad la que se equivoca. Y recuerden: ¡NO TENGA PÁNICO! (Disculpas a Douglas Adams).

Propósito y público

Este documento asume que el usuario está familiarizado con el funcionamiento de una red IP simple sin conexión (por ejemplo, algunos sistemas 4.3 BSD en una red Ethernet sin conexión a ningún otro lugar). El Apéndice A contiene información complementaria para llegar a este punto. Su propósito es que la persona, familiarizada con una red simple, se familiarice con la "tradición oral" de Internet hasta el punto de que pueda conectarse a Internet sin riesgo para ninguno de los dos. No es un tutorial, sino que contiene enlaces a otros sitios, literatura y sugerencias que normalmente no se documentan. Dado que Internet es un entorno dinámico, este documento se modificará periódicamente. El autor agradece comentarios y sugerencias, especialmente en lo que respecta a los términos del glosario (no es necesario definirlos).

¿Qué es Internet?

En sus inicios, existía ARPANET, una red experimental de área extensa que conectaba hosts y servidores de terminales. Se establecieron procedimientos para regular la asignación de direcciones y crear estándares voluntarios para la red. A medida que las redes de área local se generalizaron, muchos hosts se convirtieron en puertas de enlace a redes locales. Se desarrolló una capa de red

para permitir la interoperación de estas redes, denominada Protocolo de Internet (IP). Con el tiempo, otros grupos crearon redes de larga distancia basadas en IP (NASA, NSF, estados...). Estas redes también interoperan gracias al IP. El conjunto de todas estas redes interoperativas constituye Internet.

Unos pocos grupos proporcionan gran parte de los servicios de información en Internet. El Instituto de Ciencias de la Información (ISI) realiza gran parte del trabajo de estandarización y asignación de Internet, actuando como la Autoridad de Números Asignados de Internet (IANA). SRI International proporciona los principales servicios de información para Internet mediante la operación del Centro de Información de Red (NIC). De hecho, una vez conectado a Internet, la mayor parte de la información de este documento puede obtenerse del SRI-NIC. Bolt Beranek and Newman (BBN) proporciona servicios de información para CSNET (el CIC) y NSFNET (el NNSC), y Merit proporciona servicios de información para NSFNET (el NIS).

Operación de Internet

Cada red, ya sea ARPANET, NSFNET o una red regional, tiene su propio centro de operaciones. ARPANET está gestionada por BBN, Inc. bajo contrato con DCA (en nombre de DARPA). Sus instalaciones se denominan Centro de Operaciones de Red o NOC. Merit, Inc. opera NSFNET desde otro NOC completamente independiente. Continúa con las regionales, que cuentan con instalaciones similares para supervisar y vigilar la actividad de su parte de Internet. Además, todas deben tener algún conocimiento de lo que sucede en Internet en general. Si surge un problema, se sugiere que un enlace de la red del campus se ponga en contacto con el operador de red al que está conectado directamente. Es decir, si está conectado a una red regional (que tiene acceso a NSFNET, que a su vez está conectada a ARPANET, etc.) y tiene un problema, debe ponerse en contacto con su centro de operaciones de red regional.

RFC

El funcionamiento interno de Internet se define mediante un conjunto de documentos llamados RFC (Solicitud de Comentarios). El proceso general para crear una RFC consiste en que quien desee formalizar un documento escriba un documento que describa el problema y lo envíe por correo electrónico a Jon Postel (Postel@ISI.EDU). Él actúa como árbitro de la propuesta. Posteriormente, todos aquellos que deseen participar en la discusión la comentan (electrónicamente, por supuesto). Puede pasar por varias revisiones. Si se acepta generalmente como una buena idea, se le asignará un número y se archivará en las RFC.

Existen dos categorizaciones independientes de protocolos. La primera es el estado de la técnica. La estandarización puede ser "estándar", "borrador de estándar", "propuesto", "experimental" o "histórico". La segunda es el estado de este protocolo, que puede ser "obligatorio", "recomendado", "electivo" o "no recomendado". Se podría esperar que un protocolo en particular avance en la escala de estatus de electivo a obligatorio al mismo tiempo que avanza en la escala de estandarización de propuesto a estándar.

Un protocolo Estándar Obligatorio (por ejemplo, RFC-791, Protocolo de Internet) debe implementarse en cualquier host conectado a Internet. Los protocolos Estándar Recomendados generalmente son implementados por los hosts de red. Su ausencia no impide el acceso a Internet, pero puede afectar su usabilidad. RFC-793 (Protocolo de Control de Transmisión) es un protocolo Estándar Recomendado. Los protocolos Electivos Propuestos fueron debatidos y acordados, pero su

aplicación nunca se ha generalizado. Esto puede deberse a la falta de una amplia necesidad de la aplicación específica (RFC-937, Protocolo de Oficina Postal) o a que, aunque técnicamente superior, se oponía a otros enfoques generalizados. Se sugiere que, si un sitio en particular requiere la función, se realice una implementación de acuerdo con la RFC. Esto garantiza que, si la idea llega a su fin, la implementación se ajuste a un estándar y sea de uso general.

Las RFC informativas contienen información objetiva sobre Internet y su funcionamiento (RFC-1010, Números Asignados). Finalmente, con el desarrollo de Internet y la tecnología, algunas RFC se han vuelto innecesarias. Sin embargo, estas RFC obsoletas no pueden ignorarse. Con frecuencia, cuando se realiza un cambio en una RFC que provoca la publicación de una nueva, dejando obsoletas otras, la nueva RFC puede contener solo explicaciones y motivaciones del cambio. Comprender el modelo en el que se basa toda la función puede implicar la lectura de las RFC originales y posteriores sobre el tema. (El Apéndice B contiene una lista de las principales RFC necesarias para comprender Internet).

Solo unas pocas RFC especifican estándares; la mayoría son para fines informativos o de debate. Para conocer los estándares actuales, consulte la RFC titulada "Estándares Oficiales de Protocolo de la IAB" (publicada recientemente como RFC-1100).

El Centro de Información de Red (NIC)

El NIC es un recurso disponible para todos los usuarios de Internet que proporciona información a la comunidad. Existen tres medios de contacto con el NIC: red, teléfono y correo electrónico. Los accesos de red son los más comunes. El acceso interactivo se utiliza con frecuencia para consultar resúmenes de servicios del NIC, buscar nombres de usuario y host, y consultar listas de documentos del NIC. Está disponible mediante %telnet nic.ddn.mil

en un sistema BSD, siguiendo las instrucciones de un indicador intuitivo. Tras explorar las bases de datos proporcionadas, se podría concluir que valdría la pena tener un documento llamado NETINFO:NUG.DOC (Guía del usuario de ARPANET). Se podría recuperar mediante un FTP anónimo. Un FTP anónimo procedería de forma similar a la siguiente. (El diálogo puede variar ligeramente según la implementación de FTP que se utilice).

```
%ftp nic.ddn.mil
Conectado a nic.ddn.mil
220 NIC.DDN.MIL Servidor FTP 5Z(47)-6 el miércoles 17 de junio de 1987 a las
12:00 PDT
Nombre (nic.ddn.mil:myname): anónimo
331 Usuario anónimo ok, enviar identidad real como contraseña. Contraseña:
minombre
230 Usuario anónimo inició sesión el miércoles 17 de junio de 1987 a las 12:01
PDT, tarea 15.
ftp> get netinfo:nug.doc
200 Puerto 18.144 en el host 128.174.5.50 aceptado.
150 Recuperación ASCII de NUG.DOC.11 iniciada.
226 Transferencia completada. 157675 (8) bytes transferidos.
local: netinfo:nug.doc remoto: netinfo:nug.doc
157675 bytes en 4.5e+02 segundos (0.34 Kbytes/s)
ftp> quit
221 Comando QUIT recibido. Adiós.
```

(Otro buen documento inicial para obtener es NETINFO:WHAT-THE-NIC-DOES.TXT).

Las preguntas al NIC o los problemas con los servicios se pueden consultar o reportar mediante correo electrónico. Se pueden utilizar las siguientes direcciones:

```
NIC@NIC.DDN.MIL Asistencia general al usuario, solicitud de documentos
REGISTRAR@NIC.DDN.MIL Registro de usuarios y actualizaciones de WHOIS
HOSTMASTER@NIC.DDN.MIL Cambios y actualizaciones de nombres de host y dominios
ACTION@NIC.DDN.MIL Operaciones informáticas SRI-NIC
SUGGESTIONS@NIC.DDN.MIL Comentarios sobre publicaciones y servicios del NIC
```

Para quienes no tienen acceso a la red, o si la cantidad de documentos es grande, muchos de los documentos del NIC están disponibles en formato impreso por un pequeño costo. Un documento que se solicita con frecuencia para sitios web de inicio es un compendio de las principales RFC. El acceso telefónico se utiliza principalmente para preguntas o problemas con el acceso a la red. (Consulte el apéndice B para obtener los números de contacto por correo/teléfono).

El Centro de Servicios de Red NSFNET

El Centro de Servicios de Red NSFNET (NNSC), ubicado en BBN Systems and Technologies Corp., es un proyecto de la Corporación Universitaria para la Investigación Atmosférica en virtud de un acuerdo con la Fundación Nacional para la Ciencia.

La NNSC ofrece soporte a los usuarios finales de NSFNET si tienen preguntas o problemas al navegar por la red.

La NNSC, que cuenta con información y documentos en línea e impresos, distribuye noticias a través de listas de correo de la red, boletines e informes en línea. Las publicaciones de la NNSC incluyen un boletín impreso, NSF Network News, que contiene artículos de interés para los usuarios de la red, y la Guía de Recursos de Internet, que enumera instalaciones (como centros de supercomputación y catálogos de bibliotecas en línea) accesibles desde Internet. La Guía de Recursos se puede obtener mediante FTP anónimo a nnsc.nsf.net en el directorio resource-guide, o uniéndose a la lista de correo de la guía de recursos (envíe una solicitud de suscripción a Resource-Guide-Request@NNSC.NSF.NET).

Reflectores de correo

La mayoría de las personas se mantienen al día con las noticias de la red suscribiéndose a varios reflectores de correo (también conocidos como detonadores de correo). Los reflectores de correo son buzones electrónicos especiales que, al recibir un mensaje, lo reenvían a una lista de otros buzones. Esto crea un grupo de discusión sobre un tema específico. Cada suscriptor ve todo el correo reenviado por el reflector y, si alguien quiere aportar su opinión, le envía un mensaje con los comentarios.

El formato general para suscribirse a una lista de correo consiste en buscar la dirección del reflector y añadir la cadena -REQUEST al nombre del buzón (no al nombre del host). Por ejemplo, si desea participar en la lista de correo de NSFNET reflejada por NSFNET-INFO@MERIT.EDU, debe enviar una solicitud a NSFNET-INFO-REQUEST@MERIT.EDU. Esto puede ser una excelente estrategia, pero el problema radica en que primero debe saber que la lista existe. Si le interesa, le recomendamos leer el correo de una lista (como NSFNET-INFO) y probablemente se familiarizará con la existencia de otras. El NIC proporciona un servicio de registro para los reflectores de correo en los archivos NETINFO:INTEREST-GROUPS-1.TXT, NETINFO:INTEREST-GROUPS-2.TXT, NETINFO:INTEREST-GROUPS-3.TXT, a través de NETINFO:INTEREST-GROUPS-9.TXT.

El reflector de correo NSFNET-INFO está dirigido a quienes se interesan diariamente por las noticias de NSFNET (los trabajadores de la red troncal, la red regional y los sitios de interconexión a Internet). Los mensajes se reflejan desde una ubicación central y se envían como mensajes separados a cada suscriptor. Esto genera cientos de mensajes en las redes de área extensa (RAN), donde el ancho de banda escasea.

Hay dos maneras en que un campus podría difundir las noticias sin que estos mensajes saturen las RAN. Una es volver a reflejar el mensaje en el campus. Es decir, configurar un reflector en una máquina local que reenvíe el mensaje a una lista de distribución del campus. La otra opción es crear un alias en una máquina del campus que guarde los mensajes en un archivo de notas sobre el tema. Los usuarios del campus que deseen obtener la información pueden acceder al archivo de notas y ver los mensajes enviados desde su último acceso. También se puede optar por que el enlace de la red de área extensa del campus filtre los mensajes y reenvíe solo los que se consideren relevantes. Cualquiera de estos esquemas permite enviar un mensaje al campus, a la vez que permite una amplia distribución dentro del campus.

Asignación de direcciones

Antes de que una red local pueda conectarse a Internet, se le debe asignar una dirección IP única. Estas direcciones son asignadas por SRI-NIC. El proceso de asignación consiste en obtener un formulario de solicitud. Envíe un mensaje a Hostmaster@NIC.DDN.MIL y solicite la plantilla para una dirección conectada. Esta plantilla se completa y se envía por correo electrónico al hostmaster. Se le asigna una dirección y se le envía por correo electrónico. Esto también se puede hacer por correo postal (Apéndice B).

Las direcciones IP tienen una longitud de 32 bits. Generalmente se escribe como cuatro números decimales separados por puntos (p. ej., 192.17.5.100). Cada número es el valor de un octeto de los 32 bits. Algunas redes pueden optar por organizarse de forma muy plana (una red con muchos nodos) y otras pueden organizarse jerárquicamente (muchas redes interconectadas con menos nodos cada una y una red troncal). Para cubrir estos casos, las direcciones se diferenciaron en redes de clase A, B y C. Esta clasificación tuvo que ver con la interpretación de los octetos. Las redes de clase A tienen el primer octeto como dirección de red y los tres restantes como dirección de host en esa red. Las direcciones de clase C tienen tres octetos de dirección de red y uno de host. La clase B se divide en dos y dos. Por lo tanto, hay un espacio de direcciones para unas pocas redes grandes, una cantidad razonable de redes medianas y una gran cantidad de redes pequeñas. Los bits de orden superior en el primer octeto están codificados para indicar el formato de la dirección. Hay muy pocas redes de clase A sin asignar, por lo que es muy recomendable su uso. Por lo tanto, en la práctica, al realizar un pedido, se debe elegir entre la clase B y la clase C. (También existen formatos de clase D (multidifusión) y E (experimental). Las direcciones de multidifusión probablemente se generalicen en un futuro próximo, pero aún no se usan con frecuencia.

Anteriormente, los sitios que requerían múltiples direcciones de red solicitaban múltiples direcciones discretas (generalmente de clase C). Esto se debía a que gran parte del software disponible (en particular, 4.2BSD) no podía gestionar direcciones subdivididas en subredes. La información sobre cómo acceder a una red específica (información de enrutamiento) debe almacenarse en puertas de enlace de Internet y conmutadores de paquetes. Algunos de estos nodos tienen una capacidad limitada para almacenar e intercambiar información de enrutamiento (limitada

a unas 700 redes). Por lo tanto, se sugiere que cualquier campus anuncie (dé a conocer a Internet) no más de dos números de red discretos.

Si un campus prevé estar limitado por esto, debería considerar la subred. La subred (RFC-950) permite anunciar una dirección a Internet y utilizar un conjunto de direcciones en el campus. Básicamente, se define una máscara que permite a la red diferenciar entre la parte de red y la parte de host de la dirección. Al usar una máscara diferente en Internet y en el campus, la dirección puede interpretarse de diversas maneras. Por ejemplo, si un campus requiere dos redes internamente y tiene asignadas las 32 000 direcciones que comienzan con 128.174.X.X (una dirección de clase B), podría asignar 128.174.5.X a una parte del campus y 128.174.10.X a otra. Al anunciar 128.174 a Internet con una máscara de subred de FF.FF.00.00, Internet trataría estas dos direcciones como una sola. Dentro del campus se usaría una máscara de FF.FF.FF.00, lo que permitiría al campus tratar las direcciones como entidades separadas. (En realidad, no se pasa la máscara de subred FF.FF.00.00 a Internet; el significado del octeto está implícito en que es una dirección de clase B).

Es necesario tener en cuenta una advertencia: no todos los sistemas pueden realizar subredes. Algunos sistemas 4.2BSD requieren software adicional. La subred de los sistemas 4.3BSD se publicó. Otros dispositivos y sistemas operativos varían en los problemas que presentan al gestionar subredes. Con frecuencia, estas máquinas pueden utilizarse como una hoja en una red, pero no como una puerta de enlace dentro de la parte subdividida de la misma. Con el paso del tiempo y la incorporación de más sistemas a 4.3BSD, estos problemas deberían desaparecer.

Ha habido cierta confusión en el pasado sobre el formato de una dirección IP de difusión. Algunas máquinas utilizaban una dirección de solo ceros para indicar difusión y otras de solo unos. Esto resultaba confuso cuando máquinas de ambos tipos se conectaban a la misma red. Se ha adoptado la dirección de difusión de solo unos para solucionar este problema. Algunos sistemas (por ejemplo, 4.3BSD) permiten elegir el formato de la dirección de difusión. Si un sistema permite esta opción, se debe tener cuidado de elegir el formato de solo unos. (Esto se explica en las RFC-1009 y RFC-1010).

Problemas de Internet

Internet presenta varios problemas. Las soluciones a los problemas abarcan desde cambios de software hasta proyectos de investigación a largo plazo. Algunas de las principales se detallan a continuación:

Número de redes

Cuando se diseñó Internet, se preveía que contara con unas 50 redes conectadas. Con la explosión de las redes, la cifra se acerca a las 1000. El software de un grupo de puertas de enlace críticas (denominadas puertas de enlace centrales) no puede transmitir ni almacenar una cantidad mucho mayor. A corto plazo, la reasignación y recodificación de núcleos ha aumentado ligeramente esta cifra.

Problemas de enrutamiento

Además de la gran cantidad de datos necesarios para enrutar paquetes a un gran número de redes, existen numerosos problemas con la actualización, la estabilidad y la optimización de los algoritmos de enrutamiento. Se está investigando mucho en este campo, pero la solución óptima a estos

problemas de enrutamiento aún está a años de distancia. En la mayoría de los casos, el enrutamiento actual funciona, pero de forma deficiente y, a veces, impredecible. La mayor esperanza actual para un buen protocolo de enrutamiento es algo conocido como OSPFIGP, que estará disponible de forma generalizada a través de muchos fabricantes de enrutadores dentro de un año.

Problemas de Confianza

Las puertas de enlace intercambian información de enrutamiento de red. Actualmente, la mayoría de las puertas de enlace aceptan sin reservas que la información proporcionada sobre el estado de la red es correcta. Anteriormente, esto no representaba un gran problema, ya que la mayoría de las puertas de enlace pertenecían a una sola entidad administrativa (DARPA). Ahora, con múltiples redes de área amplia bajo diferentes administraciones, una puerta de enlace no autorizada en algún punto de la red podría paralizar Internet. Se está trabajando en el diseño para resolver tanto el problema de que una puerta de enlace cometa errores irrazonables como para proporcionar suficiente información para enrutar datos de forma razonable entre múltiples redes conectadas (redes multiconexionadas).

Capacidad y Congestión

Algunas partes de Internet sufren una gran congestión durante las horas punta del día. El crecimiento es drástico, y algunas redes experimentan un crecimiento del tráfico superior al 20 % mensual. Se planea un ancho de banda adicional, pero la entrega y los presupuestos podrían no permitir que el suministro se mantenga al ritmo.

Estableciendo Dirección y Prioridad

La Junta de Actividades de Internet (IAB), actualmente presidida por Vint Cerf de NRI, es responsable de establecer la dirección técnica, establecer estándares y resolver problemas en Internet.

Los miembros actuales del IAB son:

```
Vinton Cerf - Presidente
David Clark - Presidente del IRTF
Phillip Gross - Presidente del IETF
Jon Postel - Editor de RFC
Robert Braden - Director Ejecutivo
Hans-Werner Braun - Enlace de NSFNET
Barry Leiner - Enlace de CCIRN
Daniel Lynch - Enlace de Proveedores
Stephen Kent - Seguridad en Internet
```

Este comité cuenta con el apoyo de un Grupo de Trabajo de Investigación (presidido por Dave Clark del MIT) y un Grupo de Trabajo de Ingeniería (presidido por Phill Gross del NRI).

El Grupo de Trabajo de Investigación de Internet cuenta con los siguientes Grupos de Investigación: Redes Autónomas: Deborah Estrin Servicios de Extremo a Extremo: Bob Braden Privacidad: Steve Kent Interfaces de Usuario: Keith Lantz

El Grupo de Trabajo de Ingeniería de Internet cuenta con las siguientes áreas técnicas:

```
Aplicaciones (Por definir)
Protocolos de Host: Craig Partridge
```

```
Protocolos de Internet: Noel Chiappa
Enrutamiento: Robert Hinden
Gestión de Red: David Crocker
Interoperabilidad OSI: Ross Callon, Robert Hagen
Operaciones (Por definir)
Seguridad (Por definir)
```

El Grupo de Trabajo de Ingeniería de Internet cuenta con los siguientes Grupos de Trabajo:

```
ALERTMAN: Louis Steinberg
Autenticación: Jeff Schiller
CMIP sobre TCP: Lee LaBarre
Nombres de Dominio: Paul Mockapetris
Configuración Dinámica de Host: Ralph Droms
Requisitos de Host: Bob Braden
Interconectividad: Guy Almes
MIB de Internet: Craig Partridge
Gestión Conjunta: Susan Hares
MIB de LAN: Amatzia Ben-Artzi
NISI: Karen Bowers
Interfaz Serie NM: Jeff Case
Herramientas NOC: Bob Enger
OSPF: Mike Petry
Enrutamiento de Sistemas Abiertos: Marianne Lepp
Interoperabilidad OSI Ross Callon
Grupo de Enrutamiento PDN CH Rokitansky
Rendimiento y CC Allison Mankin
IP Punto-Punto Drew Perkins
ST y CO-IP Claudio Topolcic
Telnet Dave Borman
Documentos de Usuario Karen Roubicek
Servicios de Usuario Karen Bowers
```

Enrutamiento

El enrutamiento es el algoritmo mediante el cual una red dirige un paquete desde su origen hasta su destino. Para comprender el problema, observe a un niño pequeño intentando encontrar mesa en un restaurante. Desde la perspectiva de un adulto, se observa la estructura del comedor y se puede elegir fácilmente una ruta óptima. Sin embargo, al niño se le presentan un conjunto de rutas entre mesas donde no se puede discernir una buena ruta, ni mucho menos la óptima, hacia el objetivo.

Un poco más de contexto sería útil. Las puertas de enlace IP (o, más correctamente, los enrutadores) son dispositivos que tienen conexiones a múltiples redes y transfieren tráfico entre ellas. Deciden cómo se enviará el paquete basándose en la información del encabezado IP del paquete y el estado de la red. Cada interfaz de un enrutador tiene una dirección única, apropiada para la red a la que está conectada. La información del encabezado IP que se utiliza es principalmente la dirección de destino. Otra información (por ejemplo, el tipo de servicio) se ignora en gran medida en este momento. El estado de la red se determina mediante el intercambio de información entre los enrutadores. La distribución de la base de datos (lo que cada nodo conoce), la forma de las actualizaciones y las métricas utilizadas para medir el valor de una conexión son los parámetros que determinan las características de un protocolo de enrutamiento.

Con algunos algoritmos, cada nodo de la red tiene conocimiento completo del estado de la red (el algoritmo adulto). Esto implica que los nodos deben tener mayor cantidad de almacenamiento local y suficiente CPU para buscar en las tablas grandes en un tiempo breve (recuerde, esto debe hacerse

para cada paquete). Además, las actualizaciones de enrutamiento generalmente contienen solo cambios en la información existente (o se gasta una gran cantidad de la capacidad de la red en el intercambio de actualizaciones de enrutamiento de megabytes). Este tipo de algoritmo presenta varios problemas. Dado que la única forma en que se puede transmitir la información de enrutamiento es a través de la red y el tiempo de propagación no es trivial, la vista de la red en cada nodo es una vista histórica correcta de la red en diferentes momentos del pasado. (El algoritmo para adultos, pero en lugar de ello es más fácil elegir la ruta óptima que mirar directamente al comedor, o una fotografía del mismo. Es probable que uno elija la ruta óptima y descubra que un carrito de autobús se ha movido para bloquear el paso después de tomar la foto. Estas inconsistencias pueden causar rutas circulares (llamadas bucles de enrutamiento), donde, una vez que un paquete entra, se enruta por una ruta cerrada hasta que su campo de tiempo de vida (TTL) expira y se descarta.

Otros algoritmos pueden conocer solo un subconjunto de la red. Para evitar bucles en estos protocolos, se suelen utilizar en redes jerárquicas. Conocen completamente su propia área, pero para salir de ella se dirigen a un lugar específico (la puerta de enlace predeterminada). Normalmente se utilizan en redes más pequeñas (de campus o regionales).

Protocolos de enrutamiento en uso actual:

Estático (sin tabla de protocolos/enrutamiento predeterminado)

No se ría. Es probablemente el más fiable, el más fácil de implementar y el que menos problemas genera en una red pequeña o una hoja en Internet. Este es, además, el único método disponible en algunas combinaciones de CPU y sistema operativo. Si un host está conectado a una red Ethernet con una sola puerta de enlace, se debe establecer esta como la puerta de enlace predeterminada y no realizar ningún otro enrutamiento. (Por supuesto, esa puerta de enlace podría transmitir la información de accesibilidad de alguna manera al otro lado de sí misma).

Advertencia: solo con extrema precaución se deben utilizar rutas estáticas en medio de una red que también utiliza enrutamiento dinámico. Los enrutadores que transmiten información dinámica a veces se confunden por rutas dinámicas y estáticas conflictivas. Si su host está en una red Ethernet con varios enrutadores a otras redes y estos enrutadores realizan enrutamiento dinámico entre sí, generalmente es mejor participar en el enrutamiento dinámico que usar rutas estáticas.

RIP

RIP es un protocolo de enrutamiento basado en XNS (Xerox Network System) adaptado para redes IP. Lo utilizan muchos enrutadores (Proteon, Cisco, UB...) y muchos sistemas Unix BSD. Los sistemas BSD suelen ejecutar un programa llamado "routed" para intercambiar información con otros sistemas que ejecutan RIP. RIP funciona mejor en redes de pequeño diámetro (pocos saltos) donde los enlaces tienen la misma velocidad. Esto se debe a que la métrica utilizada para determinar la mejor ruta es el número de saltos. Un salto es un recorrido a través de una puerta de enlace. Por lo tanto, todas las máquinas en la misma Ethernet están a cero saltos de distancia. Si un enrutador conecta dos redes directamente, una máquina al otro lado del enrutador está a un salto de distancia. A medida que la información de enrutamiento pasa por una puerta de enlace, esta suma uno al número de saltos para mantener la coherencia en toda la red. El diámetro de una red se define como el mayor número de saltos posible dentro de una red. Desafortunadamente, un número de saltos de 16 se define como infinito en RIP, lo que significa que el enlace está inactivo. Por lo tanto, RIP no permitirá la comunicación entre hosts separados por más de 15 puertas de enlace en el espacio RIP.

El otro problema con las métricas de número de saltos es que, si los enlaces tienen diferentes velocidades, esa diferencia no se refleja en el número de saltos. Por lo tanto, se utilizaría un enlace satelital de un salto (con un retraso de 0,5 segundos) a 56 kb en lugar de una conexión T1 de dos saltos. La congestión puede considerarse una disminución de la eficacia de un enlace. Por lo tanto, a medida que un enlace se congestiona más, RIP seguirá sabiendo que es la ruta con mejor número de saltos y la congestionará aún más, enviando más paquetes a la cola para ese enlace.

RIP no estaba bien documentado originalmente en la comunidad, y la gente consultaba el código BSD para descubrir cómo funcionaba realmente. Finalmente, se documentó en el RFC-1058.

Router

El programa router, que realiza RIP para sistemas 4.2BSD, ofrece muchas opciones. Una de las más utilizadas es "routed -q" (modo silencioso), que significa escuchar la información RIP, pero nunca difundirla. Esto lo utilizaría una máquina en una red con múltiples puertas de enlace que utilizan RIP. Permite al host determinar qué puerta de enlace es la mejor (por saltos) para llegar a una red distante. (Por supuesto, podría ser conveniente tener una puerta de enlace predeterminada para evitar tener que pasar todas las direcciones conocidas de Internet mediante RIP).

Hay dos maneras de insertar rutas estáticas en routed: el archivo /etc/gateways y el comando "route add". Las rutas estáticas son útiles si sabe cómo acceder a una red distante, pero no la recibe mediante RIP. Generalmente, es preferible usar el comando "route add". Esto se debe a que el comando agrega la ruta a la tabla de enrutamiento de esa máquina, pero no la exporta mediante RIP. El archivo /etc/gateways tiene prioridad sobre cualquier información de enrutamiento recibida mediante una actualización de RIP. Además, se transmite como un hecho en las actualizaciones de RIP generadas por el host sin cuestionarlo, por lo que si se comete un error en el archivo /etc/gateways, este pronto se filtrará al espacio RIP y podría colapsar la red.

Uno de los problemas con routed es que tiene muy poco control sobre qué se transmite y qué no. Muchas veces, en redes grandes donde varias partes de la red están bajo diferentes controles administrativos, le gustaría transmitir a través de RIP solo las redes que recibe de RIP y que sabe que son razonables. Esto evita que se agreguen direcciones IP a la red, lo cual podría ser ilegal, y que usted sea responsable de transmitirlas a Internet. Este tipo de comprobaciones de razonabilidad no está disponible con las redes enrutadas y las mantiene utilizables, pero es inadecuado para redes grandes.

Hello (RFC-891)

Hello es un protocolo de enrutamiento diseñado e implementado en un enrutador de software experimental llamado "Fuzzball" que se ejecuta en un PDP-11. No se usa ampliamente, pero es el protocolo de enrutamiento utilizado anteriormente en la red troncal NSFNET inicial. Los datos transferidos entre nodos son similares a los de RIP (una lista de redes y sus métricas). Sin embargo, la métrica son milisegundos de retraso. Esto permite que Hello se utilice en redes de diversas velocidades de enlace y tenga un mejor rendimiento en situaciones de congestión.

Una de las ventajas más interesantes de las redes basadas en Hello es su gran capacidad de cronometraje. Si consideramos el problema de medir el retardo en un enlace para la métrica, nos damos cuenta de que no es fácil. No se puede medir el tiempo de ida y vuelta, ya que el enlace de retorno puede estar más congestionado, tener una velocidad diferente o incluso no existir. No es

viable que cada nodo de la red tenga un receptor WWV (estándar nacional de tiempo de radio) integrado. Por lo tanto, es necesario diseñar un algoritmo para transmitir el tiempo entre nodos a través de los enlaces de red, donde el retardo de transmisión solo puede ser aproximado. Los enrutadores de hola hacen esto y, en una red nacional, mantienen la sincronización horaria con una precisión de milisegundos. (Véase también el Protocolo de Tiempo de Red, RFC-1059).

Protocolo de Puerta de Enlace (GGP RFC-823)

Las puertas de enlace centrales utilizaban originalmente GGP para intercambiar información entre sí. Este es un algoritmo de "vector de distancia". Las nuevas puertas de enlace centrales utilizan un algoritmo de "estado de enlace".

NSFNET SPF (RFC-1074)

Los enrutadores troncales NSFNET actuales utilizan una versión del protocolo de enrutamiento ANSI IS-IS e ISO ES-IS. Se trata de un algoritmo de "primero la ruta más corta" (SPF), perteneciente a la clase de algoritmos de "estado de enlace".

Protocolo de Puerta de Enlace Exterior (EGP RFC-904)

EGP no es estrictamente un protocolo de enrutamiento, sino un protocolo de accesibilidad. Indica qué redes se pueden alcanzar a través de qué puerta de enlace, pero no la calidad de la conexión. Es el estándar mediante el cual las puertas de enlace intercambian información de accesibilidad de red con las puertas de enlace principales. Se utiliza generalmente entre sistemas autónomos. Existe una métrica que se transmite mediante EGP, pero su uso no está estandarizado formalmente. El valor de la métrica varía de 0 a 255, y los valores más bajos se consideran "mejores". Algunas implementaciones consideran que el valor 255 significa inaccesible. Muchos enrutadores utilizan EGP para poder interactuar con enrutadores de diferentes fabricantes o administrados por diferentes administraciones. Por ejemplo, cuando un enrutador de la red troncal de NSFNET intercambia información de enrutamiento o accesibilidad con una puerta de enlace de una red regional, se utiliza EGP.

Gated

Tenemos redes regionales y de campus que utilizan RIP entre sí, y la DDN y NSFNET utilizan EGP. ¿Cómo interoperan? Inicialmente, existía el enrutamiento estático. El problema con el enrutamiento estático en medio de la red es que se transmite a Internet, independientemente de si es utilizable. Por lo tanto, si una red se vuelve inaccesible e intenta acceder a ella, el enrutamiento dinámico emitirá inmediatamente una red inaccesible. Con el enrutamiento estático, los enrutadores pensarían que la red es accesible y continuarían intentándolo hasta que la aplicación se rindiera (en 2 minutos o más). Mark Fedor, entonces de Cornell, intentó resolver estos problemas con un sustituto de enrutado llamado gated.

Gated comunica RIP con hosts que utilizan RIP, EGP con hablantes de EGP y Hello con usuarios de Hello. Estos hablantes suelen estar todos en una misma red Ethernet, pero afortunadamente (o desafortunadamente) no pueden entender las reflexiones de los demás. Además, bajo el control del archivo de configuración, se puede filtrar la conversión. Por ejemplo, se puede generar una configuración que indique que las redes RIP se anuncien mediante Hello solo si están especificadas en una lista y también son accesibles mediante una difusión RIP. Esto significa que si una red no

autorizada aparece en el espacio RIP de su sitio local, no se transmitirá al lado Hello. También existen opciones de configuración para realizar enrutamiento estático y nombrar puertas de enlace de confianza.

Esto puede parecer la mejor tecnología desde la invención del pan rebanado, pero hay un problema: la conversión de métricas. RIP mide en saltos, Hello en milisegundos y EGP usa números pequeños arbitrarios. La pregunta clave es cuántos saltos hay en un milisegundo, cuántos milisegundos hay en el número EGP 3... Además, recuerde que el infinito (inalcanzable) es 16 para RIP, aproximadamente 30 000 para Hello y 8 para el DDN con EGP. Conseguir que todas estas métricas funcionen correctamente en conjunto no es tarea fácil. Si se hace incorrectamente y traduces un RIP de 16 a un EGP de 6, todos en ARPANET seguirán pensando que tu puerta de enlace puede alcanzar lo inalcanzable y te enviará todos los paquetes del mundo. Gated está disponible a través de FTP anónimo desde devvax.tn.cornell.edu en el directorio pub/gated.

Nombres

Todo el enrutamiento en la red se realiza mediante la dirección IP asociada a un paquete. Dado que a los humanos les resulta difícil recordar direcciones como 128.174.5.50, se creó un registro de nombres simbólicos en la NIC donde se podía decir: "Quiero que mi host se llame uiucuxc". Las máquinas conectadas a Internet en todo el país se conectaban a la NIC en plena noche, comprobaban las fechas de modificación en el archivo de hosts y, si se modificaba, lo movían a su máquina local. Con la llegada de las estaciones de trabajo y los micros, los cambios en el archivo de host debían realizarse a diario. Además, era muy laborioso y consumía mucho ancho de banda de red. El RFC-1034 y otros describen el Servicio de Nombres de Dominio (DNS), un sistema de base de datos distribuido para asignar nombres a direcciones.

Debemos analizar con más detalle el significado de un nombre. En primer lugar, cabe destacar que una dirección especifica una conexión específica en una red. Si la máquina se traslada, la dirección cambia. En segundo lugar, una máquina puede tener uno o más nombres y una o más direcciones de red (conexiones) a diferentes redes. Los nombres apuntan a algo que realiza un trabajo útil (es decir, la máquina) y las direcciones IP apuntan a una interfaz de ese proveedor. Un nombre es una representación puramente simbólica de una lista de direcciones en la red. Si una máquina se traslada a otra red, las direcciones cambiarán, pero el nombre podría permanecer igual.

Los nombres de dominio son nombres con estructura de árbol, con la raíz del árbol a la derecha. Por ejemplo:

```
uxc.cso.uiuc.edu
```

es una máquina llamada "uxc" (puramente arbitraria), dentro de los subdominios de la Universidad de Illinois y "uiuc" (la Universidad de Illinois en Urbana), registrada en "edu" (el conjunto de instituciones educativas).

Un modelo simplificado de cómo se resuelve un nombre es que en la máquina del usuario hay un resolver. Este resuelve cómo contactar con un servidor de nombres raíz a través de la red. Los servidores raíz son la base del sistema de recuperación de datos estructurado en árbol. Saben quién es responsable de gestionar los dominios de primer nivel (p. ej., 'edu'). La decisión sobre qué servidores raíz utilizar es un parámetro de instalación. Desde el servidor raíz, el resolver averigua quién proporciona el servicio 'edu'. Contacta con el servidor de nombres 'edu', que le proporciona

una lista de direcciones de servidores para los subdominios (como 'uiuc'). Esta acción se repite con los servidores de subdominios hasta que el subdominio final devuelve una lista de direcciones de interfaces en el host en cuestión. La máquina del usuario puede entonces elegir cuál de estas direcciones utilizar para la comunicación.

Un grupo puede solicitar su propio nombre de dominio (como 'uiuc', mencionado anteriormente). Esto se realiza de forma similar a la asignación de direcciones IP. Los únicos requisitos son que el solicitante tenga dos máquinas accesibles desde Internet, que actuarán como servidores de nombres para ese dominio. Estos servidores también podrían actuar como servidores para subdominios, o bien, otros servidores podrían designarse como tales. Cabe destacar que los servidores no necesitan estar ubicados en un lugar específico, siempre que sean accesibles para la resolución de nombres. (La Universidad de Illinois podría solicitar a la Universidad Estatal de Michigan que actúe en su nombre, lo cual sería un buen método). El mayor problema radica en que alguien debe realizar el mantenimiento de la base de datos. Si la máquina no es conveniente, es posible que no se realice de manera oportuna. Además, cabe destacar que, una vez asignado el dominio a una entidad administrativa, esta puede asignar libremente subdominios de la forma que considere oportuna.

El Servidor de Dominio de Nombres de Internet de Berkeley (BIND) implementa el servidor de nombres de Internet para sistemas UNIX. El servidor de nombres es un sistema de base de datos distribuido que permite a los clientes nombrar recursos y compartir esa información con otros hosts de la red. BIND está integrado con 4.3BSD y se utiliza para buscar y almacenar nombres de host, direcciones, agentes de correo, información de host y más. Reemplaza el archivo /etc/hosts o la búsqueda de nombres de host. BIND sigue siendo un programa en evolución. Para mantenerse al día con los informes sobre problemas operativos, futuras decisiones de diseño, etc., únase a la lista de correo de BIND enviando una solicitud a Bind-Request@UCBARPA.BERKELEY.EDU. BIND también se puede obtener mediante FTP anónimo desde ucbarpa.berkeley.edu.

Usar BIND ofrece varias ventajas. Una de las más importantes es que libera al host de la necesidad de que el archivo /etc/hosts esté actualizado y completo. Dentro del dominio .uiuc.edu, solo unos pocos hosts están incluidos en la tabla de hosts distribuida por SRI. El resto se lista localmente en las tablas de BIND en uxc.cso.uiuc.edu (el servidor de la mayor parte del dominio .uiuc.edu). Todos son igualmente accesibles desde cualquier otro host de Internet que ejecute BIND o cualquier sistema de resolución DNS.

BIND también puede proporcionar información de reenvío de correo para hosts internos a los que no se puede acceder directamente desde Internet. Estos hosts pueden estar en redes no anunciadas o no estar conectados a una red IP.

No funcionan en absoluto, como en el caso de los hosts accesibles mediante UUCP (véase RFC-974). Hay más información sobre BIND en la "Guía de Operaciones del Servidor de Nombres para BIND" del Manual del Administrador del Sistema UNIX, versión 4.3BSD.

Existen algunos dominios especiales en la red, como NIC.DDN.MIL, la base de datos de hosts del NIC. Existen otros con el formato NNSC.NSF.NET. Estos dominios especiales se usan con moderación y requieren una amplia justificación. Se refieren a servidores bajo el control administrativo de la red, en lugar de a una sola organización. Esto permite que el servidor real se mueva por la red mientras que la interfaz de usuario de esa máquina permanece constante. Es decir, si BBN cede el control del NNSC, el nuevo proveedor será identificado por ese nombre.

En realidad, el sistema de dominios es mucho más general y complejo de lo que se ha descrito. Los resolutores y algunos servidores almacenan información en caché para permitir omitir los pasos de la resolución. La información proporcionada por los servidores puede ser arbitraria, no solo direcciones IP. Esto permite que el sistema se utilice tanto en redes no IP como para correo, donde puede ser necesario proporcionar información sobre puentes de correo intermedios.

¿Qué problemas tiene Berkeley Unix?

La Universidad de California en Berkeley ha recibido financiación de DARPA para modificar el sistema Unix de diversas maneras. Entre estas modificaciones se incluye la compatibilidad con los protocolos de Internet. En versiones anteriores (p. ej., BSD 4.2) existía una buena compatibilidad con los protocolos básicos de Internet (TCP, IP, SMTP, ARP), lo que le permitía un buen rendimiento en redes Ethernet IP e Internet más pequeñas. Sin embargo, existían deficiencias al conectarse a redes complejas. La mayoría de estos problemas se han resuelto en la versión más reciente (BSD 4.3). Dado que es la plataforma desde la que muchos proveedores han lanzado implementaciones de Unix (ya sea adaptando el código existente o utilizándolo como modelo), muchas implementaciones (p. ej., Ultrix) todavía se basan en BSD 4.2. Por lo tanto, aún existen muchas implementaciones con los problemas de BSD 4.2. Con el tiempo, cuando BSD 4.3 se implemente gradualmente entre los proveedores como nueva versión, muchos de los problemas se resolverán. A continuación, se presenta una lista de algunos escenarios problemáticos y su gestión en cada una de estas versiones.

Redirecciones ICMP

Bajo el modelo de Internet, todo lo que un sistema necesita saber para acceder a Internet es su propia dirección, la dirección a la que desea ir y cómo llegar a una puerta de enlace que conozca Internet. No tiene que ser la mejor puerta de enlace. Si el sistema está en una red con múltiples puertas de enlace y un host envía un paquete para su entrega a una puerta de enlace que considera que otra puerta de enlace conectada directamente es más adecuada, la puerta de enlace envía al remitente un mensaje. Este mensaje es una redirección ICMP, que dice cortésmente: "Le entregaré este mensaje, pero debería usar esa puerta de enlace de allí para llegar a este host". BSD 4.2 ignora estos mensajes. Esto genera mayor estrés en las puertas de enlace y la red local, ya que por cada paquete enviado, la puerta de enlace envía un paquete al originador. BSD 4.3 utiliza la redirección para actualizar sus tablas de enrutamiento, usará la ruta hasta que se agote el tiempo de espera y luego volverá a usar la ruta que considere adecuada. Todo el proceso se repite, pero es mucho mejor que uno por paquete.

Tráilers

Una aplicación (como FTP) envía una cadena de octetos a TCP, que la divide en fragmentos y añade un encabezado TCP. TCP envía bloques de datos a IP, que añade sus propios encabezados y envía los paquetes por la red. Esta adición de encabezados a los datos provoca movimientos de memoria tanto en la máquina emisora como en la receptora. Alguien tuvo la brillante idea de que si los paquetes eran largos y se pegaban los encabezados al final (se convertían en tráileres), la máquina receptora podría colocar el paquete al principio del límite de una página y, si el tráiler era correcto, simplemente eliminarlo y transferir el control de la página sin movimientos de memoria. El problema radica en que los tráilers nunca se estandarizaron y la mayoría de las puertas de enlace no saben cómo buscar la información de enrutamiento al final del bloque. Cuando se utilizan tráilers, la

máquina suele funcionar correctamente en la red local (sin puertas de enlace involucradas) y para bloques cortos a través de puertas de enlace (en los que no se utilizan tráilers). Por lo tanto, TELNET y FTP para archivos muy cortos funcionan correctamente, mientras que los FTP para archivos largos parecen bloquearse. En BSD 4.2, los tráilers son una opción de arranque y es recomendable asegurarse de que estén desactivados al usar Internet. BSD 4.3 negocia los tráilers, por lo que los usa en su red local y no los usa al navegar por la red.

Retransmisiones

TCP envía bloques a su socio en el otro extremo de la conexión. Si no recibe una confirmación en un tiempo razonable, retransmite los bloques. El algoritmo de retransmisión de TCP determina qué es razonable.

No existe un algoritmo correcto, pero algunos son mejores que otros, donde lo peor se mide por el número de retransmisiones realizadas innecesariamente. BSD 4.2 tenía una retransmisión

Un algoritmo que retransmitía rápida y frecuentemente. Esto es justo lo que se desearía si se tuvieran varias máquinas en una red Ethernet (una red de bajo retardo y gran ancho de banda). Si se tiene una red con un retardo relativamente mayor y un ancho de banda limitado (por ejemplo, líneas de 56 kb), tiende a retransmitir de forma demasiado agresiva. Por lo tanto, obliga a las redes y puertas de enlace a pasar más tráfico del necesario para una conversación determinada. Los algoritmos de retransmisión se adaptan al retardo de la red después de unos pocos paquetes, pero el de la versión 4.2 se adapta lentamente en situaciones de retardo. BSD 4.3 funciona mucho mejor e intenta ofrecer lo mejor para ambos mundos. Inicia algunas retransmisiones muy rápidamente, asumiendo que se trata de una red de bajo retardo, y luego las detiene rápidamente. También permite que el retardo sea de unos 4 minutos antes de darse por vencido y declarar la conexión interrumpida.

Incluso mejor que el código original de la versión 4.3 es una versión de TCP con un algoritmo de retransmisión desarrollado por Van Jacobson de LBL. Investigó a fondo el funcionamiento del algoritmo en redes reales y lo modificó para obtener un mejor rendimiento y una mayor compatibilidad con la red. Este código se ha integrado en las versiones posteriores de BSD 4.3 y se puede obtener de forma anónima desde ucbarpa.berkeley.edu, en el directorio 4.3.

Tiempo de vida

La cabecera del paquete IP contiene un campo llamado tiempo de vida (TTL). Este campo se decrementa cada vez que el paquete atraviesa una puerta de enlace. El TTL se diseñó para evitar que los paquetes atrapados en bucles de enrutamiento se transmitan indefinidamente sin posibilidad de entrega. Dado que la definición se asemeja en cierta medida al número de saltos de RIP, algunos sistemas mal informados han establecido el campo TTL en 15 porque el indicador de inalcanzable en RIP es 16. Obviamente, ninguna red puede tener más de 15 saltos. El espacio RIP, donde los saltos son limitados, finaliza cuando RIP deja de utilizarse como protocolo de enrutamiento (por ejemplo, cuando NSFnet comienza a transportar el paquete). Por lo tanto, es bastante fácil que un paquete requiera más de 15 saltos. Estas máquinas mostrarán el comportamiento de poder llegar a algunos lugares pero no a otros, incluso aunque la información de enrutamiento parezca correcta.

Resolver el problema generalmente requiere parches del kernel, por lo que puede ser difícil si el código fuente no está disponible.

Apéndice A - Referencias a información correctiva

[1] Quarterman y Hoskins, "Redes informáticas notables", Communications of the ACM, vol. 29, n.º 10, págs. 932-971, octubre de 1986.

[2] Tannenbaum, A., "Redes informáticas", Prentice Hall, 1981.

[3] Hedrick, C., "Introducción a los protocolos de Internet", vía FTP anónimo desde topaz.rutgers.edu, directorio pub/tcp-ip-docs, archivo tcp-ip-intro.doc.

[4] Comer, D., "Internetworking with TCP/IP: Principles, Protocols, and Architecture", Copyright 1988, by Prentice-Hall, Inc., Englewood Cliffs, NJ, 07632 ISBN 0-13-470154-2.

Apéndice B - Lista de las principales RFC

Esta lista de las principales RFC "Basic Beige" fue compilada por J.K. Reynolds. Esta es la edición del 30 de agosto de 1989.

```
RFC-768 Protocolo de Datagramas de Usuario (UDP)
RFC-791 Protocolo de Internet (IP)
RFC-792 Protocolo de Mensajes de Control de Internet (ICMP)
RFC-793 Protocolo de Control de Transmisión (TCP)
RFC-821 Protocolo Simple de Transferencia de Correo (SMTP)
RFC-822 Estándar para el Formato de Mensajes de Texto de Internet ARPA
RFC-826 Protocolo de Resolución de Direcciones Ethernet
RFC-854 Protocolo Telnet
RFC-862 Protocolo de Eco
RFC-894 Estándar para la Transmisión de Datagramas IP a través de Redes Ethernet
RFC-904 Protocolo de Puerta de Enlace Exterior
RFC-919 Difusión de Datagramas de Internet
RFC-922 Difusión de Datagramas de Internet en Presencia de Subredes
RFC-950 Procedimiento de Subredes Estándar de Internet
RFC-951 Protocolo Bootstrap (BOOTP)
RFC-959 Protocolo de Transferencia de Archivos (FTP)
RFC-966 Grupos de Hosts: Una Extensión de Multidifusión para Protocolo de
Internet
RFC-974 Enrutamiento de correo y el sistema de dominios
RFC-1000 Guía de referencia para la solicitud de comentarios
RFC-1009 Requisitos para las puertas de enlace de Internet
RFC-1010 Números asignados
RFC-1011 Protocolos oficiales de Internet
RFC-1012 Bibliografía de la solicitud de comentarios 1 a 999
RFC-1034 Nombres de dominio: conceptos e instalaciones
RFC-1035 Nombres de dominio: implementación
RFC-1042 Estándar para la transmisión de datagramas IP sobre redes IEEE 802
RFC-1048 Extensiones de información del proveedor BOOTP
RFC-1058 Protocolo de información de enrutamiento
RFC-1059 Protocolo de tiempo de red (NTP)
RFC-1065 Estructura e identificación de la información de gestión para redes
basadas en TCP/IP
RFC-1066 Base de información de gestión para la gestión de redes basadas en
TCP/IP Internet
RFC-1084 Extensiones de información de proveedores BOOTP
RFC-1087 Ética e Internet
RFC-1095 Servicios y protocolos comunes de información de gestión sobre TCP/IP
(CMOT)
RFC-1098 Protocolo simple de administración de red (SNMP)
RFC-1100 Estándares Oficiales de Protocolo de la IAB
RFC-1101 Codificación DNS de Nombres de Red y Otros Tipos
RFC-1112 Extensiones de Host para Multidifusión IP
```

```
RFC-1117 Números de Internet
```

Nota: Esta lista es parte de una lista de RFC por tema que puede obtenerse del NIC en NETINFO:RFC-SETS.TXT (FTP anónimo, por supuesto).

La siguiente lista no es necesaria para la conexión a Internet, pero resulta útil para comprender el sistema de dominio, el sistema de correo y las puertas de enlace:

```
RFC-974 Enrutamiento de correo y el sistema de dominio
RFC-1009 Requisitos para puertas de enlace de Internet
RFC-1034 Nombres de dominio: conceptos e instalaciones
RFC-1035 Nombres de dominio: implementación y especificación
RFC-1101 Codificación DNS de nombres de red y otros tipos
```

Apéndice C: Puntos de contacto para información de red

Centro de Información de Red (NIC)

```
Centro de Información de Red DDN
SRI International, Sala EJ291
333 Ravenswood Avenue
Menlo Park, CA 94025
(800) 235-3155 o (415) 859-3695

NIC@NIC.DDN.MIL
```

Centro de Servicios de Red NSF (NNSC) NNSC BBN Systems and Technology Corporation 10 Moulton St. Cambridge, MA 02238 (617) 873-3400 NNSC@NNSC.NSF.NET

Servicio de Información de Red (NIS) de la NSF

```
NIS
Merit Inc.
Universidad de Michigan
1075 Beal Avenue
Ann Arbor, MI 48109
(313) 763-4897

INFO@NIS.NSF.NET
```

CIC

```
Centro de Coordinación e Información de CSNET
Bolt Beranek and Newman Inc.
10 Moulton Street
Cambridge, MA 02238
(617) 873-2777

INFO@SH.CS.NET
```

Glosario

Sistema Autónomo

Un conjunto de puertas de enlace bajo un único control administrativo y que utiliza procedimientos de enrutamiento compatibles y consistentes. En general, las puertas de enlace son administradas por una organización específica. Dado que una puerta de enlace está conectada a dos (o más) redes, no suele ser correcto decir que está en una red. Por ejemplo, las puertas de enlace que conectan las redes regionales a la red troncal de la NSF son gestionadas por Merit y forman un sistema autónomo. Otro ejemplo: las puertas de enlace que conectan los campus a NYSERNET son gestionadas por NYSER y forman un sistema autónomo.

Puerta de enlace principal

Las puertas de enlace más internas de Internet. Estas puertas de enlace tienen una visión completa de la accesibilidad a todas las redes conocidas en Internet. Luego, redistribuyen la información de accesibilidad a las puertas de enlace vecinas que hablan EGP. Es a partir de ellas que su agente EGP (hay uno que actúa por usted en algún lugar si puede acceder al núcleo de Internet) descubre que puede acceder a todas las redes de Internet. Esta información se le transmite mediante un mensaje de "Hola, bloqueado, RIP". Las puertas de enlace principales conectan principalmente los campus a ARPANET o interconectan ARPANET y MILNET, y son gestionadas por BBN.

Contar hasta el infinito

El síntoma de un problema de enrutamiento es que la información de enrutamiento se transmite de forma circular a través de múltiples puertas de enlace. Cada puerta de enlace incrementa la métrica según corresponda y la transmite. A medida que la métrica se transmite por el bucle, se incrementa a valores cada vez mayores hasta alcanzar el máximo del protocolo de enrutamiento utilizado, lo que generalmente indica una interrupción del enlace.

Mantener pulsado

Cuando un enrutador descubre que una ruta en la red se ha caído, anunciando que dicha ruta ha estado inactiva durante un tiempo mínimo (normalmente al menos dos minutos). Esto permite la propagación de la información de enrutamiento a través de la red y evita la formación de bucles de enrutamiento.

Horizonte dividido

Cuando un enrutador (o un grupo de enrutadores que trabajan en consorcio) acepta información de enrutamiento de múltiples redes externas, pero no transmite la información obtenida de una red externa a ninguna otra. Esto intenta evitar que se propaguen rutas falsas a una red debido a rumores o a contar hasta el infinito.

DDN

Red de Datos de Defensa: el nombre colectivo de ARPANET y MILNET. Se usa con frecuencia porque, aunque son redes separadas, sus enfoques operativos e informativos son los mismos.

Consideraciones de Seguridad

La seguridad y la protección de la privacidad son un asunto serio y, con demasiada frecuencia, no se toman medidas al respecto. Existen algunos errores de seguridad conocidos (especialmente en el control de acceso) en BSD Unix y en algunas implementaciones de servicios de red. La guía del autoestopista no aborda estos problemas (una lástima).

Dirección del autor

Ed Krol Universidad de Illinois 195 DCL 1304 West Springfield Avenue Urbana, IL 61801-4399
Teléfono: (217) 333-7886 Correo electrónico: Krol@UXC.CSO.UIUC.EDU